Социальная психология и общество
2022. Т. 13. № 1. С. 33—50
DOI: https://doi.org/10.17759/sps.2022130103
ISSN: 2221-1527 (печатный)
ISSN: 2311-7052 (online)

Social psychology and society
2022. Vol. 13, no. 1, pp. 33—50
DOI: https://doi.org/10.17759/sps.2022130103
ISSN: 2221-1527 (print)
ISSN: 2311-7052 (online)

ЭМПИРИЧЕСКИЕ ИССЛЕДОВАНИЯ
EMPIRICAL RESEARCH

Онлайн-коммуникация в социальных медиа: как опыт утраты приватности отражается на поведении пользователей

Синявская Я.Э.
ФГАОУ ВО «Национальный исследовательский университет «Высшая школа экономики» (ФГАОУ ВО «НИУ ВШЭ»),
г. Санкт-Петербург, Российская Федерация
ORCID: https://orcid.org/0000-0003-2385-3295, e-mail: ysinyawskaya@hse.ru

Цель. *Анализ связи между опытом утраты приватности в интернете и поведением пользователей по защите персональных данных.*

Контекст и актуальность. *В эпоху стремительного развития интернет-технологий вопросы безопасности пребывания в онлайн-пространстве требуют научного осмысления. Понимание факторов регуляции онлайн-поведения пользователей может способствовать выработке адекватной политики в области приватности.*

Дизайн исследования. *С помощью регрессионного анализа производится параметрическая оценка эффекта воздействия утраты приватности на использование пользователями настроек приватности. Предварительно с помощью метода мэтчинга происходит балансирование контрольной группы (N=215) и группы воздействия (N=160) по ключевым ковариатам.*

Участники. *Пользователи крупнейшей российской социальной сети «ВКонтакте», являющиеся жителями Вологды. Размер выборки — 375 человек (55% женщин) от 16 до 83 лет (Ср.=32,5; Мед.=31; SD=12,9).*

Методы (инструменты). *Используются опросные данные о наличии опыта утраты приватности и поведенческие данные о настройках приватности, полученные из аккаунтов пользователей через API автоматическими методами. Используются русскоязычные версии шкал «Склонность устанавливать социальные связи» П. Тоттерделла (и др.) и Шкала самооценки М. Розенберга.*

Результаты. *Предыдущий опыт утраты приватности не приводит к более осторожному поведению в социальной сети: пользователи уделяют внимание регулированию только одного аспекта приватности — доступа к публичным записям аккаунта. Важным фактором оказывается компетентность пользователей в области использования настроек приватности.*

Выводы. *Полученные данные свидетельствуют в пользу гипотезы о «парадоксе приватности». Поскольку наличие конкретных навыков регулирования приватности онлайн способствует более осторожному поведению в Сети, интервенции в области цифровой грамотности могут повысить безопасность пребывания на сайтах социальных сетей.*

Ключевые слова: *социальные сети, приватность, онлайн-поведение, парадокс приватности, эффект воздействия, мэтчинг.*

Финансирование. Исследование осуществлено в рамках Программы фундаментальных исследований НИУ ВШЭ.

Для цитаты: *Синявская Я.Э.* Онлайн-коммуникация в социальных медиа: как опыт утраты приватности отражается на поведении пользователей // Социальная психология и общество. 2022. Том 13. № 1. С. 33—50. DOI:https://doi.org/10.17759/sps.2022130103

Online Social Media Communication: the Effect of Having Privacy Violation Experience on Online Behavior

Yadviga E. Sinyavskaya
National Research University Higher School of Economics, Saint Petersburg, Russia
ORCID: https://orcid.org/0000-0003-2385-3295, e-mail: ysinyawskaya@hse.ru

Objective. *To analyze the effect of privacy violation experience on privacy-protective behaviors*
Background. *In the era of rapid development of Internet technologies, privacy issues call for scientific reflection. Understanding the factors that regulate online user behavior might assist in elaborating the adequate privacy policy.*
Study design. *Regression analysis provides a parametric evaluation of the effect of privacy experience on usage of privacy settings. Various matching technics were applied for preliminary balancing of the control (N=215) and treatment groups (N=160) by a set of key covariates.*
Participants. *Users of the largest Russian online social network VKontakte from the Russian city Vologda. The sample size is 375 respondents (55% female) from 16 to 83 age (Mean=32,5; Med.=31; SD=12,9).*
Measurements. *Both survey data on privacy experience and observed behavioral data on privacy settings from users' online accounts were used. Additionally, the scale of P. Totterdell & D. Holman on propensity to make social connection and M. Rosenberg's self-esteem scale were adopted in the study*
Results. *The experience of privacy violation does not lead to the cautious behavior online: the users tend to regulate only the access to the public posts on profile due to past bad experience. The privacy settings literacy turns significantly affect the usage of privacy settings.*
Conclusions. *The findings support the "privacy paradox" hypothesis. As having specific online privacy management skills encourages more cautious behavior online, digital literacy interventions can improve the safety of social networking sites.*

Keywords: *online social networks, privacy, online behavior, privacy paradox.*

Funding. The study was implemented in the framework of the Basic Research Program at the HSE University.

For citation: Sinyavskaya Y.E. Online Social Media Communication: the Effect of Having Privacy Violation Experience on Online Behavior. *Sotsial'naya psikhologiya i obshchestvo = Social Psychology and Society*, 2022. Vol. 13, no. 1, pp. 33—50. DOI:https://doi.org/10.17759/sps.2022130103 (In Russ.).

Введение

Социальные медиа предоставляют широкие возможности для «нетворкинга» и коммуникации и рассматриваются как платформа для развития особой формы социального капитала [31].

Поскольку обмен информацией и раскрытие личных данных составляют основу коммуникации на сайтах социальных сетей [27], остро встает вопрос безопасности и сохранения приватности пользователей. Недавние прецеденты утечки персональных данных [19] и негативная динамика роста киберпреступлений последних лет [5] указывают на уязвимую позицию пользователей социальных сетей.

Опросы населения как в России [1][1], так и за рубежом [18] показывают, что пользователи выражают обеспокоенность проблемой безопасности личных данных в интернете. Однако признание важности рисков не приводит к снижению уровня онлайн-активности [7].

Сохранение безопасности и приватности тесно связано с благополучием человека [35]. Понимание факторов, регулирующих поведение пользователей социальных сетей в отношении защиты собственной приватности, может способствовать разработке адекватной политики приватности.

Наиболее разработанный подход, представленный в исследованиях, исходит из предпосылки, что восприятие риска утраты приватности (perceived risk) или обеспокоенность вопросами приватности (privacy concerns) сподвигают людей к защитным действиям («privacy protective behavior»).

Однако эмпирические исследования указывают на неоднозначность данной взаимосвязи. Так, С. Барнс был описан феномен «парадокса приватности» — противоречия между декларируемыми пользователями установками относительно важности сохранения приватности и «открытым» поведением в Сети [8].

На сегодняшний день исследователи расходятся во мнении относительно существования и природы данного феномена [15; 29]. Некоторые исследователи относят данный феномен к методологическому артефакту, указывая, что различия в концептуализации и измерении ключевых понятий приводят к существенным расхождениям в результатах [29].

Тот факт, что установки пользователей в отношении приватности нестабильно предсказывают «защитное» поведение, отнюдь не уникален для рассматриваемой предметной области. В социально-психологической литературе данная проблема была сформулирована еще в начале 20-го века и получила название «attitude-behavior gap» [30].

Альтернативный подход для объяснения и предсказания приватного поведения апеллирует к так называемой «experience-behavior» гипотезе, в рамках которой изучается влияние предыдущего опыта на последующее поведение [51].

Изучение опыта жертв природных катастроф показало, что подобные события мотивируют людей снижать вовлеченность в практики риска и стимулируют к соблюдению превентивных мер безопасности — «precautionary behavior» [36]. На сегодняшний день были обнаружены немногочисленные попытки воспроизвести данный результат в контексте изучения онлайн-приватности [14; 50].

Цель данного исследования — рассмотреть, как связь между опытом утраты приватности и приватным поведением пользователей в социальных сетях проявляется в российском контексте. Принимая во внимание многомерность данного конструкта [11], в исследовании рассматривается конкретный аспект — социальная приватность, подразумевающая регулирование режима коммуникации с другими людьми, в том числе возможность не быть втянутым в нежелательную коммуникацию.

Основная гипотеза исследования состоит в том, что наличие опыта утраты приватности в Сети будет повышать вероятность использования пользователем настроек приватности.

---

[1] Данные из исследования, проведенного «Левада-Центр». С 05.09.2016 «Левада-Центр» включен в реестр некоммерческих организаций, выполняющих функции иностранного агента

В исследовании используются наблюдаемые поведенческие данные о настройках приватности, полученные из аккаунтов пользователей социальной сети «ВКонтакте», что позволяет преодолеть ограничения самоотчетных данных, отмеченных в предыдущих исследованиях [29].

Организация и методы исследования

Выборка и данные. Представленное в статье исследование является частью проекта Лаборатории социальной и когнитивной информатики НИУ ВШЭ СПБ[2]. Дизайн исследовательского проекта был одобрен этической комиссией НИУ ВШЭ. В фокусе внимания исследования находится выборка пользователей крупнейшей российской социальной сети «ВКонтакте» [7], репрезентирующая жителей Вологды как среднестатистического по уровню социально-экономического развития [6][3] и уровню проникновения интернета города России [4].

Размер генеральной совокупности составил 196000 человек [45], размер итоговой выборочной совокупности — 375 человек (доверительный интервал — 95%, ошибка выборки — 5,3%). Часть данных была получена в ходе онлайн-опроса, часть — с помощью автоматизированной закачки серверных данных (через API запросы).

Переменные.

1) Воздействующая переменная — наличие опыта утраты приватности в социальной сети «ВКонтакте». В ходе онлайн-опроса респонденты сообщали о наличии или отсутствии опыта нарушения их приватности в Сети, выбирая из предложенного перечня различных рисков приватности [47]. В дальнейшем полученные данные были агрегированы в одну переменную, которая принимала значение «1» в случае, если респондент отметил, что хотя бы один аспект его приватности был нарушен в прошлом, и значение «0» — если данный опыт отсутствует. Таким образом, в группе воздействия (есть опыт) оказалось 160 чел., в контрольной группе (нет опыта) — 215 чел.

2) Зависимые переменные — использование настроек приватности в социальной сети «ВКонтакте». Оценивалось, как пользователь контролирует возможность других пользователей, не входящих в список онлайн-друзей, вступать с ним в коммуникацию или иметь доступ к информации на его странице (бинарные переменные, 0 — позволяет, 1 — не позволяет):

— видеть публичные посты, размещенные в профиле (36% не ограничивают данную возможность);

— оставлять публичные записи в профиле (только 10,6% респондентов предоставили данную возможность);

— комментировать публичные посты (81,6% респондентов не ограничивают данную возможность);

— отправлять запрос на добавление в друзья (89% респондентов не ограничивают данную возможность);

— вступать в личную переписку (77,8% респондентов не ограничивают данную возможность);

---

[2] Исследовательский проект Лаборатории СКИЛА НИУ ВШЭ, «Социальный капитал и приватность онлайн: городское сообщество в социальной сети». С материалами проекта можно ознакомиться по адресу: scila.hse.ru/subproject1-2017

[3] 26 место из 85 по уровню ВРП среди регионов России [6, с. 30].

— отображать онлайн-страницу в онлайн-поисковых системах (Яндекс, Гугл и др.) (37,6% не заблокировали для незнакомых людей возможность найти их персональную страницу в «ВКонтакте»);

— видеть информацию профиля (57% респондентов закрыли доступ к информации профиля).

3) Контрольные переменные:

Использование социальной сети «ВКонтакте» для коммерческих целей

Поведение пользователей, использующих личный аккаунт для коммерческих целей, может характеризоваться большей «открытостью» по сравнению с типичными пользователями социальных сетей. Респондентам было предложено оценить степень согласия со следующим утверждением: «Я использую "ВКонтакте" для продажи товаров или услуг, развития онлайн-сообществ, для коммерческих целей или продвижения себя как специалиста» (где «1» — абсолютно не согласен, «5» — полностью согласен). Далее данная переменная была дихотомизирована по медианному значению. Оказалось, что 37% респондентов используют аккаунт для личного продвижения.

Уровень цифровой грамотности

Одним из объяснений парадокса приватности, предложенным в литературе, является некомпетентность пользователей в области менеджмента настроек приватности в социальных сетях [37]. В данном исследовании респонденты отвечали на вопрос «Меняли ли Вы когда-нибудь настройки приватности в социальной сети "ВКонтакте"?». Респонденты, указавшие, что не знают про настройки приватности либо не умеют ими пользоваться, попали в группу «низкая компетенция в области использования настроек приватности» (23%).

Самооценка

В предыдущих исследованиях было показано, что низкий уровень самооценки может быть связан с низким контролем приватности онлайн [13].

В качестве контроля в рамках измерения склонности индивида оценивать себя негативно респондентам было предложено оценить по шкале Р. Лайкерта степень согласия со следующим утверждением, адаптированным из шкалы М. Розенберга [41]: «Временами я чувствую себя никчемным». Ранее в исследовании Р. Робинс и коллег [40] было показано, что такой психологический конструкт, как самооценка [41], может быть аппроксимирован с помощью одного вопроса с удовлетворительными показателями качества.

Склонность устанавливать связи с другими людьми

В предыдущих исследованиях было показано, что уровень экстраверсии связан со степенью самораскрытия индивидов онлайн [12]. В исследовании была адаптирована методика П. Тоттерделла и др. [49], оценивающая стремление индивида устанавливать новые социальные связи.

Согласно результатам конфирматорного факторного анализа отражающая теоретические представления о факторной структуре инструмента трехфакторная модель демонстрирует приемлемые показатели соответствия по всем индексам [10] ($\chi 2$=964,32; p=0,00; CFI=0,996; TLI=0,991; RMSEA=0,039). Надежность субшкал варьируется в пределах от 0.65 до 0.78, что находится в рамках установленной нормы [46]. Графический анализ кривой ответов (Category response curves, CRC) [37] показал, что вопросы осмысленно предсказывают, какую категорию ответов выберет индивид с определенным уровнем выраженности фактора Склонность устанавливать социальные связи.

Социально-демографические данные

Респондентам задавался ряд вопросов об их социально-демографическом статусе: возрасте, поле, уровне образования и роде занятий. Оказалось, что выборка на 55% состоит из женщин, средний возраст респондентов — 32,5 года (мин.=14, макс.=83, медиана=31, станд. откл.=12,9). Около трети респондентов имеют незаконченное высшее образование (30,7%), 9% имеют законченное высшее образование. Большинство респондентов работают в коммерческом секторе или являются самозанятыми (32,8%), 11,2% задействованы в государственном секторе, а 17,9% выбрали опцию «Другое».

Методика анализа данных

Выводы исследования основываются на параметрической оценке среднего эффекта воздействия опыта, связанного с утратой приватности, на использование индивидом настроек приватности (estimation of average treatment effect). Идея оценки среднего эффекта развита в трудах Д. Рубина [43] и восходит к теории контрфактуального вывода и оценки возможных/потенциальных исходов (potential/counterfactual outcomes). Формальное описание данного подхода представлено ниже.

Пусть для всех индивидов в выборке i=1, N определено множество двух возможных исходов $\{Y_i(0)Y_i(1)\}$ вследствие воздействия T, где исход $Y_i(1)$ наступает, если индивид i использует настройки приватности, исход $Y_i(0)$ указывает на неиспользование пользователем настроек приватности:

$$Y_i = Y_i(T_i) = \begin{cases} Y_{i-}(0), \text{если } T_i = 0 \\ Y_i(1), \text{если } T_i = 1 \end{cases}$$

Таким образом, каждого индивида в выборке можно отнести либо к группе воздействия, либо к контрольной группе в зависимости от типа воздействия и наблюдаемого исхода.

Идея контрфактуальных исходов предлагает рассматривать наряду с наблюдаемыми исходами, представленными в выборке, и так называемые контрфактуальные (потенциальные) исходы, которые описывают некий альтернативный для индивида исход в гипотетической ситуации, если бы воздействие на него не было (или было) оказано в зависимости от наблюдаемого исхода [23]. Таким образом, если предполагается одновременное рассмотрение обоих исходов для индивида, когда он подвергся (исход $Y_i(1)$) и не подвергся воздействию (исход $Y_i(0)$), то индивидуальный эффект воздействия представляет собой разность этих исходов $Y_i(1) - Y_i(0)$.

Средний эффект воздействия (Sample Average Treatment Effect) представляет собой сумму разностей всех индивидуальных исходов:

$$\text{SATE} = \frac{1}{n} \sum_{i=1}^{n} [\text{Y}_\text{i}(1) - \text{Y}_\text{i}(0)],$$

где i — число наблюдений, для которых Ti=1.

Чтобы воссоздать ненаблюдаемый исход для каждого индивида (counterfactual outcome) и устранить дисбаланс в значении ковариат в контрольной и экспериментальной группах, используются техники так называемого мэтчинга — специального метода сопоставления наблюдений в выборке [44].

Несмотря на отдельные попытки сформулировать общие рекомендации по выбору подходящего метода мэтчинга [46], перебор и тестирова-

ние различных методов предлагаются в качестве универсальной рекомендации [21]. Тем не менее при выборе методов мэтчинга кажется важным принять во внимание дискуссию, существующую между представителями двух конкурирующих подходов — доминирующего в литературе подхода Equal percent bias reducing (EPBR) [43] и нового класса методов «Monotonic Imbalance Bounding» (MIB) [25]. Ключевые различия между данными подходами заключаются, во-первых, в принципах сопоставления наблюдений в выборке и объединения их в мэтчинг-пару и, во-вторых, в алгоритмах, с помощью которых достигается баланс данных.

Подробный анализ и тестирование существующих техник мэтчинга находятся за рамками данного исследования, однако кажется важным обеспечить некоторую сравнительную перспективу при выборе методов мэтчинга, сопоставив результаты нескольких наиболее разработанных методов в рамках конкурирующих подходов.

Из спектра методов первого подхода была выбрана наиболее популярная в социальных науках техника мэтчинга [52], оценивающая «расстояния» между наблюдениями по методу «ближайшего соседа» (nearest neighborhood, NN). В качестве критерия для определения степени близости двух наблюдений на пространстве ковариат использовалось расстояние Махаланобиса [42], в соответствии с которым расстояние (D) между наблюдениями определяется как:

$$D_{ij} = \left(x_i - x_j\right)' \Sigma^{-1} \left(x_i - x_j\right),$$

где Σ — ковариационная матрица ковариат [3].

Особенностью данной метрики является ее независимость от используемых единиц измерения переменных [3], что является преимуществом для работы с имеющимся набором данных, в котором переменные измерены в разных шкалах. Важным параметром также является количество наблюдений из противоположной группы, которое ставится в соответствие объекту. Согласно [3], универсальных рекомендаций в данном отношении не выработано, и зачастую один объект для соответствия считается достаточным.

Из пула стратификационных методов был рассмотрен метод Coarsened exact мэтчинг [26], который является модификацией наиболее простого и мощного мэтчинг метода — exact matching [21], адаптированного для работы с континуальными переменными. В основе данного метода лежит работа по формированию страт, репрезентирующих всевозможные комбинации значений рассматриваемых ковариат, и отнесение наблюдения к той или иной страте.

Исходя из специфики работы выбранных методов можно предположить, что первый метод приведет к меньшим потерям данных при более низких показателях итоговой сбалансированности и к обратной ситуации в случае второго метода.

Предварительная подготовка и диагностика данных для мэтчинга

Предварительная диагностика данных показала, что распределение переменной *уровень образования* сильно отклоняется от нормального, что осложняет ее использование для мэтчинга с расстоянием Махаланобиса, который является чувствительным к распределению переменных [22]. Номинальная переменная *род деятельности* трудно

поддается редукции до более простых категорий, что осложняет ее использование для Coarsened exact мэтчинга. Дальнейшая проверка показала, что данные переменные не оказывают влияние на целевую переменную. Поскольку относительно данных переменных не было выдвинуто теоретических ожиданий, было принято решение исключить их из перечня переменных.

Анализ данных

С помощью метода логистической регрессии производится параметрическая оценка эффекта воздействия опыта утраты приватности на использование пользователями настроек приватности. Для оценки адекватности полученных моделей данным (goodness-of-fit statistics) используется ряд показателей pseudo R2 [34] (NagelKerke, McFadden, Cox and Snell). Дополнительно для оценки качества модели использовался тест Хосмера-Лемешова, значимость которого ($p<0,05$) указывает на низкое качество модели [24]. Наконец, информационный критерий AIC (Akaike's Information Criteria) рассматривается как основа для сравнения моделей между собой, где более низкие значения указывают на лучшее качество модели [9]. Обработка и анализ данных были проведены с помощью языка программирования R (в среде Rstudio, версия 3.6.1.) с использованием пакетов MatchIt, Cem, rcompanion, generalhoslem, psych, mirt, lavaan.

Результаты

Предварительная диагностика исходных данных показала, что по всем переменным, кроме возраста и склонности устанавливать связи, разница в средних значениях между группой воздействия и контрольной группой является незначимой и не превышает 0,08, что указывает на удовлетворительную сбалансированность исходных данных (табл. 1). Балансировка данных позволила устранить различия в средних значениях между всеми переменными.

Полученные регрессионные модели демонстрируют удовлетворительное качество [33], показатели псевдо-R2 варьируются в диапазоне 0,1-0,5 (табл. 2). Однако как показатели псевдо-R2, так и информационные критерии AIC показывают, что модели, построенные на сбалансированных данных, демонстрируют более высокое качество, чем модель с исходными данными. Тесты Хосмера-Лемешова оказываются незначимыми, что позволяет отвергнуть нулевую гипотезу о неудовлетворительном качестве моделей. Как и ожидалось, наивысшее качество демонстрирует CEM-модель, однако она же характеризуется большей потерей данных.

В ходе регрессионного моделирования удалось выявить средний эффект воздействия переменной «Опыт утраты приватности» только на один тип поведения по поддержанию приватности — ограничение доступа к входящим постам на стене. Созвучно исследованию [37], вторым фактором, демонстрирующим устойчивую взаимосвязь с данной зависимой переменной, оказывается цифровая грамотность пользователя в вопросах защиты приватности.

Обсуждение результатов

Вопросы защиты личной приватности и безопасности в интернете оказываются

Таблица 1

Разница в средних значениях показателей в контрольной группе и группе воздействия при использовании различных техник мэтчинга данных

Переменные	Исходный дисбаланс		Мэтчинг по методу «ближайшего соседа» (nearest neighborhood, NN) с применением расстояния Махаланобиса		Мэтчинг по методу поиска приближенно-точных соответствий (Coarsened exact, CEM)	
Возраст	-3,07**		-1.7		0,01	
Пол	0,04		0,01		0,00	
Использование социальной сети для профессиональных целей	0,06		0,006		0,00	
Склонность устанавливать связи	0,21*		0,11		0,00	
Цифровая грамотность	0,02		0,006		0,00	
Самооценка	0,08		0,09		0,00	
Дистанция	0,03		-		-0,002	
N (В=группа воздействия; К=контрольная группа)	В=215	К=160	В=160	К=160	В=150	К=122

Примечания: * — p<0.05, ** — p<0.01; *** — p<0.001.

релевантны для респондентов — приватность практически половины респондентов (43%) была нарушена ранее в том или ином аспекте.

Несмотря на данную статистику, регулирование только одного аспекта приватности определяется предыдущим опытом — доступ других людей к записям, размещенным на стене в профиле пользователя в социальной сети «ВКонтакте», что в некоторой степени совпадает с результатами предыдущих исследований (приложение 1).

Полученные результаты до некоторой степени согласуются с «experience-behavior» гипотезой [51], рассматривающей предыдущий опыт как основу для последующего поведения. Получается, что именно возможность просмотра постов, оставленных другими людьми на стене, ассоциируется у пользователей с рисками для приватности и требует регулирования (в то время как комментирование и написание постов на стене таковым не является).

В целом «стена» является важным каналом для публичной коммуникации пользователя с аудиторией своих подписчиков [31], где пользователи общаются и получают обратную связь друг от друга. В то же самое время посты, оставленные другими пользователями публично, могут стать источником риска приватности по нескольким причинам. Во-первых, в одном виртуальном пространстве смешивается множество различных социальных контекстов индивида, что приводит к так называемому «контекстуальному коллапсу» [17]. Данный феномен описывается как ситуация, в которой индивид вынужден учитывать присутствие в одном виртуальном пространстве совершенно разных «аудиторий»

(коллеги, родственники, друзья и т.д.), с каждой из которых могут быть различные по степени близости отношения. В дополнение, в отсутствие ограничений настроек приватности у пользователей отсутствует возможность контролировать содержание и момент появления входящей информации на стене, которая потенциально может повлечь для человека репутационные или иные риски.

Следует отметить, что нерегулирование других рассмотренных аспектов приватности может быть связано с их большей значимостью для нетворкинга и целей построения социального капитала. Теория «privacy calculus» предлагает рассматривать решения индивидов в отношении поддержания личной приватности онлайн с экономических позиций: пользователи взвешивают возможные выгоды и последствия, следующие за раскрытием какой-либо информации, и выбирают вариант, при котором выгоды превышают «потери» [16]. В контексте данной теории выгода от нерегулирования рассмотренных аспектов приватности может перевешивать возможные риски. Прояснение значимости данных аспектов онлайн-поведения для выстраивания стратегий онлайн-презентации и нетворкинга пользователей кажется интересной перспективой для дальнейших исследований.

Текущее исследование не выявило значимой связи между открытостью постов на стене пользователя и стремлением развивать социальные связи. Можно предположить, что посты других пользователей на стене воспринимаются менее продуктивной основой для развития социального капитала, нежели личная информация. Кроме того, различия в результатах могут следовать из концептуальной разницы в измерении социальной активности индивида. В текущем исследовании данный конструкт рассматривался больше как поведенческая ориентация, нежели чем личностная черта [28].

В одной из моделей обнаруживаются гендерные различия, созвучные с полученными на выборках пользователей социальной сети «Фейсбук»[4]: женщины оказываются менее склонны регулировать доступ к публичным записям профиля [20]. Данные различия могут интерпретироваться в терминах «цифрового разрыва», который возникает в связи с различиями в гендерной социализации и влияет на степень владения техническими навыками, в том числе в области защиты цифровых персональных данных [38].

Ограничения исследования

Одно из ограничений связано с методикой построения выборки в онлайн-исследованиях, надежность которых активно обсуждается в научном сообществе [2]. Несмотря на оптимистические оценки метода поточной выборки, данная техника, как и традиционные, не освобождает от смещений, связанных с самоотбором (self-selection bias). Размер данного смещения невозможно оценить, поскольку отсутствует техническая возможность получить сведения о тех людях, которые увидели, но не совершили переход по ссылке рекламного объявления.

[4] С 21 марта 2022 года официально запрещен на территории России.

Данные об используемых настройках приватности и наличии у пользователя негативного опыта утраты приватности принадлежат к одному временному периоду. Кроме того, рассматривалось естественное, а не контролируемое влияние воздействующей переменной на возможные поведенческие исходы. Несмотря на использование методов псевдорандомизации, до некоторой степени позволяющих отделить эффект негативного опыта на поведение пользователей от эффектов других переменных, полученные результаты следует интерпретировать в терминах взаимосвязи, а не каузальности.

Дополнительно следует отметить, что шкала склонности устанавливать социальные связи ранее не была адаптирована на русский язык и нуждается в более детальном изучении и валидации. Переменная «Самооценка» измерялась одним вопросом, что также ограничивает возможности интерпретации связанного с ней эффекта. Дополнительная проверка показала устойчивость полученных эффектов при исключении из анализа данных измерений, что позволяет исключить негативное влияние их неустановленного статуса валидности на итоговый результат.

Наконец, в фокусе внимания исследования находятся пользователи конкретной социальной сети, являющиеся жителями определенного города России, что также ограничивает потенциал для генерализации полученных результатов.

Выводы

Полученные результаты можно обобщить в следующих выводах:

1. Наличие у пользователя опыта, связанного с нарушением его приватности в социальной сети, практически не приводит к более «бдительному» поведению. Единственный аспект приватности, который является значимым для пользователей — доступ к публичным записям, размещенным в аккаунте пользователя. Таким образом, наблюдается выборочное действие так называемого «парадокса приватности», когда негативный опыт приводит к частичному регулированию собственной безопасности онлайн.

2. Использование настроек приватности пользователем связано с его информированностью о возможностях поддержания приватности, предоставляемых социальной сетью. Таким образом, различные интервенции в области повышения цифровой грамотности пользователей могут оказаться эффективным способом повышения безопасности пребывания в Сети.

3. В исследовании применялись различные техники мэтчинга, позволяющие сбалансировать существующие данные и выявить эффект воздействия негативного опыта на поведение в области приватности. Методологические различия рассмотренных техник мэтчинга проявились только на уровне качества полученных моделей, однако не привели к содержательным различиям в результатах исследования.

Таблица 2

Модели логистической регрессии, описывающие эффект воздействия негативного опыта приватности на доступ к записям на стене пользователя

Переменные	Модель 1 без контрольных переменных (несбаланс. данные)			Модель 2 с контрольными переменными (несбаланс. данные)			Модель 3 мэтчинг по методу «ближайшего соседа» (nearest neighborhood, NN) с применением расстояния Махаланобиса			Модель 4 мэтчинг по методу поиска приближенно-точных соответствий (Coarsened exact, CEM)		
	Est	**SE**	**OR**	**Est**	**SE**	**OR**	**Est**	**SE**	**OR**	**Est**	**SE**	**OR**
Значение свободного члена регрессии	0,4***	0,11	0,55	0,5***	0,12	1,61	0,5**	0,14	1,64	0,7***	0,17	1,98
Опыт утраты приватности (нет)	**-0,11***	**0,04**	**0,89**	**-0,11***	**0,05**	**0,89**	**-0,1(.)**	**0,05**	**0,9**	**-0,11***	**0,05**	**0,9**
Возраст				0,00	0,02	1,00	0,001	0,05	1.00	0,001	0,05	1,00
Пол (муж.)				-0,0	0,05	0,93	-0,05	0,05	1,05	**-0,12***	**0,05**	**0,88**
Использование социальной сети для профессиональных целей (нет)				0,04	0,05	1,05	-0,08	0,05	0,92	0,01	0,06	1,01
Склонность устанавливать социальные связи				0,03	0,02	1,03	0,02	0,02	1,02	0,05	0,06	1,06
Цифровая грамотность (низкая)				**-0,18****	**0,07**	**0,82**	**-0.18***	**0,07**	**0,83**	**-0,34****	**0,11**	**0,7**
Самооценка				0,01	0,01	1,01	0,001	0,02	1,01	**0,15(.)**	**0,09**	**1,17**
Размер выборки	375			375			320			272		
Псевдо-R2 Нагелькерке (Nagelkerke pseudo-R2)	0.014			0,05			0,31			0.5		
Псевдо-R2 МакФаддена (McFadden pseudo-R2)	0.009			0.036			0.25			0.31		
Псевдо-R2 Кокса и Снелла (Cox and Snell pseudo-R2)	0.013			0.049			0.18			0.45		
Результаты теста Хосмера–Лемешева (Hosmer-Lemeshov test)	p=1			p=0,67			p=0,35			p=0,36		
Информационный критерий Акаике (AIC)	513			511			435			366		

Примечания: * — p<0.05, ** — p<0.01, *** — p<0.001.

Приложение 1

Сравнительный анализ результатов исследований о связи между опытом утраты онлайн-приватности и поведением пользователей социальных сетей

Поведение: практики регулирования приватности	Результаты предыдущих исследований	Результаты текущего исследования
Состав друзей	Отрицательная взаимосвязь [33]	Не обнаружено взаимосвязи
Информация профиля	• Отрицательная взаимосвязь [33] • Не обнаружено взаимосвязи [34]	Не обнаружено взаимосвязи
Публичные записи (комментирование)	Не обнаружено взаимосвязи [34]	Не обнаружено взаимосвязи
Публичные записи (написание)	Не обнаружено взаимосвязи [34]	Не обнаружено взаимосвязи
Публичные записи (просмотр)	-	Отрицательная взаимосвязь
Личные сообщения («direct communication»)	-	Не обнаружено взаимосвязи
Отображение профиля в поисковых системах	-	Не обнаружено взаимосвязи

Литература

1. Безопасность личных данных. Левада-центр [Электронный ресурс]. URL: www.levada.ru/2017/05/25/bezopasnost-personalnyh-dannyh/ (дата обращения: 21.09.2020).
2. *Девятко И.Ф.*, Экономики В.Ш. Онлайн-исследования и методология социальных наук: новые горизонты, новые (и не столь новые) трудности // Онлайн-исследования в России 2.0.: сб. статей / Под ред. Шашкина А.В., Девятко И.Ф., Давыдова С.Г. М.: РИЦ «Северо-Восток», 2010. С. 17—30.
3. *Ениколопов Р.* Оценивание эффекта воздействия // Квантиль. 2009. № 6. С. 3—15.
4. Интернет в России: динамика проникновения. Зима 2017—2018 [Электронный ресурс]. Фонд общественного мнения. URL: https://fom.ru/SMI-i-internet/13999 (дата обращения: 20.09.2020).
5. Комплексный анализ состояния преступности в Российской Федерации и расчетные варианты ее развития [Электронный ресурс] / Ю.М. Антонян [и др.]. URL: https://mvd.ru/upload/site163/document_text/Kompleksnyy_analiz__original-maket_24_04.pdf (дата обращения: 21.09.2020).
6. Регионы России. Социально-экономические показатели. Федеральная служба государственной статистики. Москва: Росстат. 2019 [Электронный ресурс]. URL: https://rosstat.gov.ru/storage/mediabank/Region_Pokaz_2019.pdf (дата обращения: 21.09.2020).
7. Социальные сети в России: цифры и тренды, осень 2019. Brand Analytics [Электронный ресурс]. URL: https://br-analytics.ru/blog/social-media-russia-2019/ (дата обращения: 21.09.2020).
8. *Barnes S.B.* A Privacy Paradox: Social Networking in the Unites States [Электронный ресурс] // First Monday. 2006. Vol. 11(9). URL: https://firstmonday.org/ojs/index.php/fm/article/view/1394 (дата обращения: 09.08.2020).

9. *Bozdogan H.* Model selection and Akaike's information criterion (AIC): The general theory and its analytical extensions // Psychometrika. 1987. Vol. 52(3). P. 345—370.
10. *Brown T.A.* Confirmatory Factor Analysis for Applied Research. NY: Guilford, 1st.ed., 2008. 462 p.
11. *Burgoon J.K.* Privacy and Communication // Communication Yearbook / In Burgoon M. (Ed.). CA.: Sage, 1982. P. 206—249.
12. *Chen B., Marcus J.* Students' self-presentation on Facebook: An examination of personality and self-construal factors // Computers in Human Behavior. 2012. Vol. 28(6). P. 2091—2099.
13. *Christofides E., Muise A., Desmarais S.* Hey mom, what's on your Facebook? Comparing Facebook disclosure and privacy in adolescents and adults // Social Psychological and Personality Science. 2012. Vol. 3(1). P. 48—54.
14. *Christofides E., Muise A., Desmarais S.* Risky disclosures on Facebook: The effect of having a bad experience on online behavior // Journal of adolescent research. 2012. Vol. 27(6). P. 714—731.
15. *Dienlin T., Trepte S.* Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors // European journal of social psychology. 2015. Vol. 45(3). P. 285—297.
16. *Dienlin T., Metzger M.J.* An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample // Journal of Computer-Mediated Communication. 2016. Vol. 21(5). P. 368—383.
17. *Donath J.S., Boyd D.* Public displays of connection // BT technology Journal. 2004. Vol. 22(4). P. 71—82.
18. Eurobarometer. Attitudes on Data Protection and Electronic Identity in the European Union. Brussels: European Commission. 2010 [Электронный ресурс]. URL: http://ec.europa.eu/public_opinion/archives/ebs/ebs_335_en.pdf (дата обращения: 21.09.2020).
19. Federal Trade Commission. FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook [Электронный ресурс]. URL: www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions (дата обращения: 20.09.2020).
20. *Gerber N., Gerber P., Volkamer M.* Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior // Computers and Security. 2018. Vol. 77. P. 226—261. DOI:10.1016/j.cose.2018.04.002
21. *Greifer N.* Matching methods. 2020 [Электронный ресурс]. URL: https://cran.r-project.org/web/packages/MatchIt/vignettes/matching-methods.html#choosing-a-matching-method/ (дата обращения: 02.02.2021).
22. *Gu X.S., Rosenbaum P.R.* Comparison of multivariate matching methods: Structures, distances, and algorithms // Journal of Computational and Graphical Statistics. 1993. Vol. 2(4). P. 405—420.
23. *Hernán M.A, Robins J.M.* Causal Inference: What if. Boca Raton: Chapman and Hall/CRC, 1 st.ed., 2020. 302 p.
24. *Hosmer D.W., Lemeshow S.* Applied Logistic Regression. New York: Wiley, 3 st.ed., 2013. 528 p.
25. *Iacus S.M., King G., Porro G.* Multivariate matching methods that are monotonic imbalance bounding // Journal of the American Statistical Association. 2011. Vol. 106(493). P. 345—361.
26. *Iacus S.M., King G., Porro G.* Causal inference without balance checking: Coarsened exact matching // Political analysis. 2012. P. 1—24.
27. *Ibrahim Y.* The new risk communities: Social networking sites and risk // International Journal of Media and Cultural Politics. 2008. Vol. 4(2). P. 245—253. DOI:10.1386/macp.4.2.245_
28. *Kalish Y., Robins G.* Psychological predispositions and network structure: The relationship between individual predispositions, structural holes and network closure // Social Networks. 2006. Vol. 28. P. 56—84. DOI:10.1016/j.socnet.2005.04.004
29. *Kokolakis S.* Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon // Computers and Security. 2017. Vol. 64. P. 122—134. DOI:10.1016/j.cose.2015.07.002

30. *LaPiere R.T.* Attitudes vs. actions // Social forces. 1934. Vol. 13(2). P. 230—237.
31. *Lee E., Kim Y.J., Ahn J.* How do people use Facebook features to manage social capital? // Computers in Human Behavior. 2014. Vol. 36. P. 440—445.
32. *Liu D., Ainsworth S.E., Baumeister R.F.* A meta-analysis of social networking online and social capital // Review of general psychology. 2016. Vol. 20(4). P. 369—391. DOI:10.1037/gpr0000091
33. *Louviere J.J., Hensher D.A., Swait J.D.* Stated choice methods: analysis and applications. Cambridge University press, 1 st. ed., 2000. 402 p.
34. *Nagelkerke N.* A note on a general definition of the coefficient of determination // Biometrika, 1991. Vol. 78. P. 691—692.
35. *Newell P.B.* Perspectives on Privacy // Journal of Environmental Psychology. 1995. Vol. 15. P. 87—104.
36. *Norris F.H., Smith T., Kaniasty K.* Revisiting the Experience—Behavior Hypothesis: The Effects of Hurricane Hugo on Hazard Preparedness and Other Self-Protective Acts // Basic and Applied Social Psychology. 1999. Vol. 21(1). P. 37—47. DOI:10.1207/s15324834basp2101_4
37. *Park Y.J.* Digital literacy and privacy behavior online // Communication Research. 2013. Vol. 40(2). P. 215—236.
38. *Park Y.J.* Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet // Computers in Human Behavior. 2015. Vol. 50. P. 252—258. DOI:10.1016/j.chb.2015.04.011
39. *Reeve B.B., Fayers P.* Applying item response theory modeling for evaluating questionnaire item and scale properties // Assessing quality of life in clinical trials: methods of practice. 2005. Vol. 2. P. 55—73.
40. *Robins R.W., Hendin H.M., Trzesniewski K.H.* Measuring global self-esteem: Construct validation of a single-item measure and the Rosenberg Self-Esteem Scale // Personality and social psychology bulletin. 2001. Vol. 27(2). P. 151—161.
41. *Rosenberg M.* Society and the adolescent self-image. Princeton, New Jersey: Princeton University Press, 1965. 338 p.
42. *Rubin D.B.* Bias Reduction Using Mahalanobis-Metric Matching // Biometrics. 1980. Vol. 36(2). P. 293—298. DOI:10.2307/2529981
43. *Rubin D.B.* Estimating causal effects of treatments in randomized and nonrandomized studies // Journal of Educational Psychology. 1974. Vol. 66. P. 688—701.
44. *Rubin D.B.* Matching to remove bias in observational studies // Biometrics. 1973. Vol. 29. P. 159—183.
45. *Rykov Y., Koltsova O., Sinyavskaya Y.* Effects of user behaviors on accumulation of social capital in an online social network // Plos one. 2020. Vol. 15(4). DOI:e0231837
46. *Stuart E.A.* Matching methods for causal inference: A review and a look forward // Statistical science: a review journal of the Institute of Mathematical Statistics. 2010. Vol. 25(1). P. 1—21.
47. *Stutzman F., Vitak J., Ellison N.B., Gray R., Lampe C.* Privacy in interaction: Exploring disclosure and social capital in Facebook // In Sixth international AAAI conference on weblogs and social media (Dublin, Ireland, June 4—7, 2012). Palo Alto: AAAI Press. Vol. 6(1).
48. *Tavakol M., Dennick R.* Making sense of Cronbach's alpha // International Journal of Medical Education. 2011. Vol. 2. P. 53—55. DOI:10.5116/ijme.4dfb.8dfd
49. *Totterdell P., Holman D., Hukin A.* Social networkers: Measuring and examining individual differences in propensity to connect with others // Social Networks. 2008. Vol. 30. P. 283—296. DOI:10.1016/j.socnet.2008.04.003
50. *Trepte S., Dienlin T., Reinecke L.* Risky behaviors: How online experiences influence privacy behaviors // From the Gutenberg galaxy to the Google galaxy / In Stark B., Quiring O., Jackob N. (Ed.). Germany: UVK Verlag, 2014. 370 p.
51. *Weinstein N.* Effects of personal experience on self-protective behavior // Psychological Bulletin. 1989. Vol. 105. P. 31—50.
52. *Zakrison T.L., Austin P.C., McCredie V.A.* A systematic review of propensity score methods in the acute care surgery literature: avoiding the pitfalls and proposing a set of reporting guidelines // European Journal of Trauma and Emergency Surgery. 2018. Vol. 44(3). P. 385—395.

References

1. Bezopasnost' lichnykh dannykh [Elektronnyi resurs] [Security of personal data]. Levada-tsentr [Levada Center]. URL: www.levada.ru/2017/05/25/bezopasnost-personalnyh-dannyh/ (Accessed 21.09.2020). (In Russ.).
2. Devyatko I.F. Onlain issledovaniya i metodologiya sotsial'nykh nauk: novye gorizonty, novye (i ne stol' novye) trudnosti [Online Research and Social Science Methodology: New Horizons, New (and Not So New) Challenges]. In Shashkina A.V. (eds.) Onlain issledovaniya v Rossi 2.0: sb. statei [Online research in Russia 2.0.]. Moscow: Publ. Severo-Vostok, 2010, pp. 17—30. (In Russ.).
3. Enikolopov R. Otsenivanie effekta vozdeistviya [The estimation of average treatment effect]. *Kvantil' = Quantile*, 2009, no. 6, pp. 3—15. (In Russ.).
4. Internet v Rossii: dinamika proniknoveniya. Zima 2017—2018 [Elektronnyi resurs] [Internet in Russia: dynamics of penetration. Winter 2017-2018]. Fond obshchestvennogo mneniya [Public Opinion Fund]. URL: https://fom.ru/SMI-i-internet/13999 (Accessed 20.09.2020). (In Russ.).
5. Kompleksnyi analiz sostoyaniya prestupnosti v Rossiiskoi Federatsii i raschetnye varianty ee razvitiya [Elektronnyi resurs] [Comprehensive analysis of the state of crime in the Russian Federation and estimated options for its development]. Yu.M. Antonyan [i dr.]. URL: https://mvd.ru/upload/site163/document_text/Kompleksnyy_analiz__original-maket_24_04.pdf (Accessed 21.09.2020). (In Russ.).
6. Regiony Rossii. Sotsial'no-ekonomicheskie pokazateli [Regions of Russia. Socio-economic indicators]. Moscow: Federal State Statistics Service, 2017, no. 32, p. 1402. (In Russ.).
7. Sotsial'nye seti v Rossii: tsifry i trendy, osen' 2019 [Elektronnyi resurs] [Social networks in Russia: numbers and trends, Fall 2019]. Brand Analytics. URL: https://br-analytics.ru/blog/social-media-russia-2019/ (Accessed 21.09.2020). (In Russ.).
8. Barnes S.B. A Privacy Paradox: Social Networking in the Unites States [Elektronnyi resurs]. *First Monday*, 2006. Vol. 11(9). URL: https://firstmonday.org/ojs/index.php/fm/article/view/1394 (Accessed 09.08.2020).
9. Bozdogan H. Model selection and Akaike's information criterion (AIC): The general theory and its analytical extensions. *Psychometrika*, 1987. Vol. 52(3), pp. 345—370.
10. Brown T.A. Confirmatory Factor Analysis for Applied Research. NY: Guilford, 1 st.ed., 2008. 462 p.
11. Burgoon J.K. Privacy and Communication. In: *Communication Yearbook*. Burgoon M. (Ed.). CA.: Sage, 1982, pp. 206—249.
12. Chen B., Marcus J. Students' self-presentation on Facebook: An examination of personality and self-construal factors. *Computers in Human Behavior*, 2012. Vol. 28(6), pp. 2091—2099.
13. Christofides E., Muise A., Desmarais S. Hey mom, what's on your Facebook? Comparing Facebook disclosure and privacy in adolescents and adults. *Social Psychological and Personality Science*, 2012. Vol. 3(1), pp. 48—54.
14. Christofides E., Muise A., Desmarais S. Risky disclosures on Facebook: The effect of having a bad experience on online behavior. *Journal of adolescent research*, 2012. Vol. 27(6), pp. 714—731.
15. Dienlin T., Trepte S. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European journal of social psychology*, 2015. Vol. 45(3), pp. 285—297.
16. Dienlin T., Metzger M.J. An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. *Journal of Computer-Mediated Communication*, 2016. Vol. 21(5), p. 368—383.
17. Donath J.S., Boyd D. Public displays of connection. *BT technology Journa*, 2004. Vol. 22(4), pp. 71—82.
18. Eurobarometer. Attitudes on Data Protection and Electronic Identity in the European Union. Brussels: European Commission. 2010 [Elektronnyi resurs]. URL: http://ec.europa.eu/public_opinion/archives/ebs/ebs_335_en.pdf (Accessed 21.09.2020).

19. Federal Trade Commission. FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook [Elektronnyi resurs]. URL: www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions (Accessed 20.09.2020).
20. Gerber N., Gerber P., Volkamer M. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers and Security,* 2018. Vol. 77, pp. 226—261. DOI:10.1016/j.cose.2018.04.002
21. Greifer N. Matching methods. 2020 [Elektronnyi resurs]. URL: https://cran.r-project.org/web/packages/MatchIt/vignettes/matching-methods.html#choosing-a-matching-method/ (Accessed 02.02.2021).
22. Gu X.S., Rosenbaum P.R. Comparison of multivariate matching methods: Structures, distances, and algorithms. *Journal of Computational and Graphical Statistics,* 1993. Vol. 2(4), pp. 405—420.
23. Hernán M.A., Robins J.M. Causal Inference: What if. Boca Raton: Chapman & Hall/CRC, 1 st.ed., 2020. 302 p.
24. Hosmer D.W., Lemeshow S. Applied Logistic Regression. New York: Wiley, 3 st.ed., 2013. 528 p.
25. Iacus S.M., King G., Porro G. Multivariate matching methods that are monotonic imbalance bounding. *Journal of the American Statistical Association*, 2011. Vol. 106(493), pp. 345—361.
26. Iacus S.M., King G., Porro G. Causal inference without balance checking: Coarsened exact matching. *Political analysis*, 2012, pp. 1—24.
27. Ibrahim Y. The new risk communities: Social networking sites and risk. *International. Journal of Media and Cultural Politics*, 2008. Vol. 4(2), pp. 245—253. DOI:10.1386/macp.4.2.245_
28. Kalish Y., Robins G. Psychological predispositions and network structure: The relationship between individual predispositions, structural holes and network closure. *Social Networks,* 2006. Vol. 28, pp. 56—84. DOI:10.1016/j.socnet.2005.04.004
29. Kokolakis S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security*, 2017. Vol. 64, pp. 122—134. DOI:10.1016/j.cose.2015.07.002
30. LaPiere R.T. Attitudes vs. actions. *Social forces*, 1934. Vol. 13(2), pp. 230—237.
31. Lee E., Kim Y.J., Ahn J. How do people use Facebook features to manage social capital? *Computers in Human Behavior*, 2014. Vol. 36, pp. 440—445.
32. Liu D., Ainsworth S.E., Baumeister R.F. A meta-analysis of social networking online and social capital. *Review of general psychology*, 2016. Vol. 20(4), pp. 369—391. DOI:10.1037/gpr0000091
33. Louviere J.J., Hensher D.A., Swait J.D. Stated choice methods: analysis and applications. Cambridge University press, 1 st.ed., 2000. 402 p.
34. Nagelkerke N. A note on a general definition of the coefficient of determination. *Biometrika*, 1991. Vol. 78, pp. 691—692.
35. Newell P.B. Perspectives on Privacy. *Journal of Environmental Psychology*, 1995. Vol. 15, pp. 87—104.
36. Norris F.H., Smith T., Kaniasty K. Revisiting the Experience—Behavior Hypothesis: The Effects of Hurricane Hugo on Hazard Preparedness and Other Self-Protective Acts. *Basic and Applied Social Psychology*, 1999. Vol. 21(1), pp. 37—47. DOI:10.1207/s15324834basp2101_4
37. Park Y.J. Digital literacy and privacy behavior online. *Communication Research*, 2013. Vol. 40(2), pp. 215—236.
38. Park Y.J. Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet. *Computers in Human Behavior*, 2015. Vol. 50, pp. 252—258. DOI:10.1016/j.chb.2015.04.011
39. Reeve B.B., Fayers P. Applying item response theory modeling for evaluating questionnaire item and scale properties. A*ssessing quality of life in clinical trials: methods of practice,* 2005. Vol. 2, pp. 55—73.
40. Robins R.W., Hendin H.M., Trzesniewski K.H. Measuring global self-esteem: Construct validation of a single-item measure and the Rosenberg Self-Esteem Scale. *Personality and social psychology bulletin*, 2001. Vol. 27(2), pp. 151—161.

41. Rosenberg M. Society and the adolescent self-image. Princeton, New Jersey: Princeton University Press, 1965. 338 p.
42. Rubin D.B. Bias Reduction Using Mahalanobis-Metric Matching. *Biometrics*, 1980. Vol. 36(2), pp. 293—298. DOI:10.2307/2529981
43. Rubin D.B. Estimating causal effects of treatments in randomized and nonrandomized studies. *Journal of Educational Psychology*, 1974. Vol. 66, pp. 688—701.
44. Rubin D.B. Matching to remove bias in observational studies. *Biometrics,* 1973. Vol. 29, pp. 159—183.
45. Rykov Y., Koltsova O., Sinyavskaya Y. Effects of user behaviors on accumulation of social capital in an online social network. *Plos one,* 2020. Vol. 15(4). DOI:e0231837
46. Stuart E.A. Matching methods for causal inference: A review and a look forward. *Statistical science: a review journal of the Institute of Mathematical Statistics*, 2010. Vol. 25(1), pp. 1—21.
47. Stutzman F., Vitak J., Ellison N.B., Gray R., Lampe C. Privacy in interaction: Exploring disclosure and social capital in Facebook. In: *Sixth international AAAI conference on weblogs and social media* (Dublin, Ireland, June 4—7, 2012). Palo Alto: AAAI Press, 2012. Vol. 6(1).
48. Tavakol M., Dennick R. Making sense of Cronbach's alpha. *International Journal of Medical Education,* 2011. Vol. 2, pp. 53—55. DOI:10.5116/ijme.4dfb.8dfd
49. Totterdell P., Holman D., Hukin A. Social networkers: Measuring and examining individual differences in propensity to connect with others. *Social Networks*, 2008. Vol. 30, pp. 283—296. DOI:10.1016/j.socnet.2008.04.003
50. Trepte S., Dienlin T., Reinecke L. Risky behaviors: How online experiences influence privacy behaviors. From the Gutenberg galaxy to the Google galaxy. In Stark B., Quiring O., Jackob N. (Ed.). Germany: UVK Verlag, 2014. 370 p.
51. Weinstein N. Effects of personal experience on self-protective behavior. *Psychological Bulletin*, 1989. Vol. 105, pp. 31—50.
52. Zakrison T.L., Austin P.C., McCredie V.A. A systematic review of propensity score methods in the acute care surgery literature: avoiding the pitfalls and proposing a set of reporting guidelines. *European Journal of Trauma and Emergency Surgery*, 2018. Vol. 44(3), pp. 385—395.

Информация об авторах
Синявская Ядвига Эдуардовна, младший научный сотрудник лаборатории социальной и когнитивной информатики, Санкт-Петербургская школа социальных наук и востоковедения, ФГАОУ ВО «Национальный исследовательский университет «Высшая школа экономики» (ФГАОУ ВО «НИУ ВШЭ»), г. Санкт-Петербург, Российская Федерация, ORCID: https://orcid.org/0000-0003-2385-3295, e-mail: ysinyawskaya@hse.ru

Information about the authors
Yadviga E. Sinyavskaya, Junior Researcher Fellow, Laboratory for Social and Cognitive Informatics, Saint-Petersburg School of Social Sciences and Area Studies, National Research University Higher School of Economics, St. Petersburg, Russia, ORCID: https://orcid.org/0000-0003-2385-3295, e-mail: ysinyawskaya@hse.ru

Получена 11.09.2020
Принята в печать 28.01.2022

Received 11.09.2020
Accepted 28.01.2022